L20: Entry 1 of 1 File: USPT May 1, 2001

must cite

US-PAT-NO: 6226618
DOCUMENT-IDENTIFIER: US 6226618 B1

TITLE: Electronic content delivery system

DATE-ISSUED: May 1, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Downs; Edgar	Fort Lauderdale	FL		
Gruse; George Gregory	Lighthouse Point	FL		
Hurtado; Marco M.	Boca Raton	FL		
Lehman; Christopher T.	Delray Beach	FL		
Milsted; Kenneth Louis	Boynton Beach	FL		
Lotspiech; Jeffrey B.	San Jose	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 09/ 133519 [PALM]
DATE FILED: August 13, 1998

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATIONS This non-provisional application claims subject matter that is technically related to the following applications that are commonly assigned herewith to International Business Machines (IBM). APPLI- CATION ATTORNEY SERIAL TITLE OF THE DOC. NO. NO. INVENTION INVENTOR(S) SE9-98-006 09/152,756 Secure Electronic Kenneth L. Milsted Content George Gregory Gruse Management Marco M. Hurtado Edgar Downs Cesar Medina SE9-98-007 09/209,440 Multimedia Player George Gregory Gruse Toolkit John J. Dorak, Jr. Kenneth L. Milsted SE9-98-008 09/241,276 Multimedia Content Kenneth L. Milsted Creation System Qing Gong Edgar Downs SE9-98-009 09/177,096 System for Tracking George Gregory Gruse End-User Electronic John J. Dorak, Jr. Content Kenneth L. Milsted SE9-98-010 09/203,307 Key Management Jeffrey B. Lotspiech System for End- Marco M. Hurtado User Digital Player George Gregory Gruse Kenneth L. Milsted SE9-98-011 09/208,774 Multi-media player Marco M. Hurtado for an Electronic George Gregory Gruse Content Delivery Edgar Downs System Kenneth L. Milsted SE9-98-013 09/203,306 A method to Kenneth L. Milsted identify CD content Craig Kindell Qing Gong SE9-98-014 09/203,315 Toolkit for Richard Spagna delivering electronic Kenneth L. Milsted content from an David P. Lybrand Online store. Edgar Downs SE9-98-015 09/201,622 A method and Kenneth L. Milsted apparatus to Kha Kinh Nguyen automatically create Qing Gong encode audio SE9-98-016 A method and Kenneth L. Milsted apparatus to Qing Gong indicate an encoding rate for audio

☐				
☐	5892900	April 1999	Ginter et al.	
☐	5915025	December 1999	Taguchi et al.	380/44
☐	5982892	November 1999	Hicks et al.	705/71
☐	5991399	November 1999	Graunke et al.	380/279
☐	5999629	December 1999	Heer et al.	705/51

OTHER PUBLICATIONS

J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures", RFC 1421, Feb., 1993, pp. 1-37.
S. Kent, "Privacy Enhancement or Internet Electronic Mail: Part II: Certificate-Based Key Management". RFC 1422, Feb., 1993, pp. 1-28.
D. Balenson, "Privace Enhancement for Internet Mail: Part III: Algorithms, Modes, and Indentifiers", RFC 1423, Feb. 1993, pp. 1-13.
B. Kaliski, "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services", RFC 1424, Feb. 1993, pp. 1-8.

ART-UNIT: 274

PRIMARY-EXAMINER: Trammell; James P.

ASSISTANT-EXAMINER: Nguyen; Nga B.

ATTY-AGENT-FIRM: Meyers; Steven J. Soucar; Steven J. Fleit, Kain, Gibbons, Gutman & Bongini P.L.

ABSTRACT:

Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system, the method comprising the steps of: transferring the encrypted data decrypting key to a clearing house that possesses a first private key, which corresponds to the first public key; decrypting the data decrypting key using the first private key; re-encrypting the data decrypting key using a second public key; transferring the re-encrypted data decrypting key to the user's system, the user's system possessing a second private key, which corresponds to the second public key; and decrypting the re-encrypted data decrypting key using the second private key.

26 Claims, 20 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 1 of 1 File: USPT May 1, 2001

DOCUMENT-IDENTIFIER: US 6226618 B1
TITLE: Electronic content delivery system

Abstract Text (1):
Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system, the method comprising the steps of: transferring the encrypted data decrypting key to a clearing house that possesses a first private key, which corresponds to the first public key; decrypting the data decrypting key using the first private key; re-encrypting the data decrypting key using a second public key; transferring the re-encrypted data decrypting key to the user's system, the user's system possessing a second private key, which corresponds to the second public key; and decrypting the re-encrypted data decrypting key using the second private key.

Brief Summary Text (12):
Briefly, in accordance with the present invention, disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system, the method comprising the steps of: transferring the encrypted data decrypting key to a clearing house that possesses a first private key, which corresponds to the first public key; decrypting the data decrypting key using the first private key; re-encrypting the data decrypting key using ia second public key; transferring the re-encrypted data decrypting key to the user's system, the user's system possessing a second private key, which corresponds to the second public key; and decrypting the re-encrypted data decrypting key using the second private key.

cl. 280

Detailed Description Text (146):
Either a Key Identifier to indicate the public encryption key that was used to encrypt the part or an encrypted symmetric key that, when decrypted, is used to decrypt the encrypted part.

Detailed Description Text (163):
If there are any changes required to be made to the watermarking instructions by the Clearinghouse(s) 105, then the Clearinghouse(s) 105 decrypts the Symmetric Key 623 and then modifies the watermarking instructions and encrypts them again using a new Symmetric Key 623. The Symmetric Key 623 is then re-encrypted using the Public Key 661 of the End-User Device(s) 109. The Clearinghouse(s) 105 also decrypts the other Symmetric Keys 623 in the SC(s) and encrypts them again with the Public Key 661 of the End-User Device(s) 109. The Clearinghouse(s) 105 builds a License SC(s) 660 that includes the newly encrypted Symmetric Keys 623 and updated watermarking instructions and sends it to the End-User Device(s) 109 in response to the Order SC (s) 650. If the processing of the Order SC(s) 650 does not complete successfully, then the Clearinghouse(s) 105 returns to the End-User Device(s) 109 an HTML page reporting the failure of the authorization process.

Detailed Description Text (175):
Watermarking Instructions--A part that contains the encrypted instructions and parameters for implementing watermarking in the Content 113. The watermarking instructions may be modified by the Clearinghouse(s) 105 and returned back to the End-User Device(s) 109 within the License SC(s) 660. There is a record in the Key Description part that defines the encryption algorithm that was used to encrypt the watermarking instructions, the output part name to use when the watermarking instructions are decrypted, a base64 encoding of the encrypted Symmetric Key 623 bitstring that is was used to encrypt the watermarking instructions, the encryption algorithm that was used to encrypt the Symmetric Key 623, and the identification of the public key that is required to decrypt the Symmetric Key 623.

Detailed Description Text (220):
The following table shows the parts that are included in the License SC(s) 660 as well as its BOM. As shown in the Key Description part, the Symmetric Keys 623 that are required for decrypting the watermarking instructions, Content 113, and Content 113 metadata have been re-encrypted by the Clearinghouse(s) 105 using the End-User (s)' Public Key 661. When the End-User Device(s) 109 receives the License SC(s) 660 it decrypts the Symmetric Keys 623 and use them to access the encrypted parts from the License SC(s) 660 and the Content SC(s) 630.

Detailed Description Text (319):
One Symmetric Key 623 is used for decrypting the watermarking instructions and the other for decrypting the Content 113 and any encrypted metadata. The watermarking instructions are included within the Metadata SC(s) 620 portion in the Order SC(s) 650. The Content 113 and encrypted metadata are in the Content SC(s) 630 at a Content Hosting Site(s) 111. The URL and part names of the encrypted Content 113 and metadata parts, within the Content SC(s) 630, are included in the Key Description part of the Metadata SC(s) 620 portion of the Order SC(s) 650. The Clearinghouse(s) 105 uses its private key to decrypt the Symmetric Keys 623 and then encrypts each of them using the Public Key 661 of the End-User Device(s) 109. The Public Key 661 of the End-User Device(s) 109 is retrieved from the Order SC(s) 650. The new encrypted Symmetric Keys 623 is included in the Key Description part of the License SC(s) 660 that the Clearinghouse(s) 105 returns to the End-User Device(s) 109.

CLAIMS:

4. The method as defined in claim 3, wherein the second encrypting key is a public key of the clearinghouse and the second decrypting key is a corresponding private key of the clearinghouse.

5. The method as defined in claim 4, wherein the step of transferring the decrypted first decrypting key includes the sub-steps of:

re-encrypting the first decrypting key using a third encrypting key, the third encrypting key being a public key of the user;

transferring the decrypted and re-encrypted first decrypting key to the user's system; and

decrypting the re-encrypted first decrypting key using a third decrypting key, the third decrypting key being a corresponding private key of the user.

11. A method of securely providing data to a user's system, the data being encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system, said method comprising the steps of:

transferring the encrypted data decrypting key to a clearing house that possesses a first private key, which corresponds to the first public key;

decrypting the data decrypting key using the first private key;

re-encrypting the data decrypting key using a second public key;

transferring the re-encrypted data decrypting key to the user's system, the user's system possessing a second private key, which corresponds to the second public key; and

decrypting the re-encrypted data decrypting key using the second private key.

17. A method of operating a clearinghouse to provide integrity in a channel of commerce that includes a provider, a distributor, and a purchaser, the provider producing data and encrypting the data so as to only be decryptable by a data decrypting key, the encrypted data being accessible to the purchaser, said method comprising the steps of:

encrypting the data decrypting key using a public key of the clearinghouse;

sending the encrypted data decrypting key from the provider to the distributor;

when the purchaser desires to purchase the data or a license to use the data, sending the encrypted data decrypting key from the distributor to the purchaser;

sending the encrypted data decrypting key from the purchaser to the clearing house;

decrypting the data decrypting key using a private key of the clearinghouse and re-encrypting the data decrypting key using a public key of the purchaser; and

sending the re-encrypted data decrypting key from the clearinghouse to the purchaser.

21. A system for securely providing data to a user's system, the system comprising:

a content system;

a first public key;

a first private key; which corresponds to the first public key;

a data encrypting key;

a data de-encrypting key for de-encrypting data encrypted using the data encrypting key;

first data encryption means for encrypting data so as to be decryptable only by a data decrypting key;

second data encryption means, using the first public key, for encrypting the decrypting key;

a clearing house;

first transferring means for transferring the data decrypting key which has been encrypted to the clearing house, wherein the clearinghouse possesses the first private key;

first decrypting means for decrypting the data decrypting key using the first private key;

a second public key;

a second private key; which corresponds to the second public key;

re-encryption means for re-encrypting the data decrypting key using the second public key;

second transferring means for transferring the re-encrypted data decrypting key to the user's system, wherein the user's system possesses the second private key; and

second decrypting means for decrypting the re-encrypted data decrypting key using the second private key.

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

End of Result Set

Generate Collection Print

L17: Entry 1 of 1 File: USPT Aug 13, 2002

US-PAT-NO: 6434535
DOCUMENT-IDENTIFIER: US 6434535 B1
**** See image for Certificate of Correction ****

TITLE: System for prepayment of electronic content using removable media and for prevention of unauthorized copying of same

DATE-ISSUED: August 13, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kupka; Michael S.	Nacogdoches	TX		
Lundgren; Michael G.	Salt Lake City	UT		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Iomega Corporation		UT			02

APPL-NO: 09/ 191976 [PALM]
DATE FILED: November 13, 1998

INT-CL: [07] G06 F 17/00

US-CL-ISSUED: 705/24; 380/228
US-CL-CURRENT: 705/24; 380/228

FIELD-OF-SEARCH: 705/41, 705/17, 705/56, 705/52, 705/53, 380/24, 380/201, 380/202, 380/228, 713/193

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4785361	November 1988	Brotby	
☐	4977594	December 1990	Shear	380/4
☐	5010571	April 1991	Katznelson	380/4
☐	5050213	September 1991	Shear	380/25
☐	5058162	October 1991	Santon et al.	380/25

0 561 685	September 1993	EP
0 665 486	August 1995	EP
0 679 980	November 1995	EP
2000010876	January 2000	JP
WO 96/35158	November 1996	WO
WO 97/14087	April 1997	WO
WO 97/29416	August 1997	WO
WO 98/02793	January 1998	WO
WO 98/43398	October 1998	WO

OTHER PUBLICATIONS

Derwent-Acc-No: 2000-147924, Horstmann, C. S., May 2001.*
Patent Abstracts of Japan, JP 10 333769 A, published Dec. 18, 1998, vol. 99(3), 1 page.

ART-UNIT: 2161

PRIMARY-EXAMINER: Sough; Hyung-sub

ASSISTANT-EXAMINER: Elisca; Pierre E.

ATTY-AGENT-FIRM: Woodcock Washburn LLP

ABSTRACT:

A system and method for distribution of electronic content over a network infrastructure and compensation of vendors of such data using prepaid media that includes a client device for operation by a user desiring to receive the electronic content and server that contains the electronic content and offering the electronic content for downloading to the client device via the network infrastructure. The client device communicates a unique identifier associated with a particular piece of media to which the electronic content is to be stored to the server. The server contacts a media tracking sever to determine if the media is valid and a remaining balance of the prepaid media. The cost of the electronic content to be downloaded is deducted from the remaining balance and credited to the vendor's account. The server then encrypts the electronic content using the unique identifier as a key and downloads the encrypted electronic content to the client computer, where the client computer writes the encrypted electronic content to the particular piece of media such that the encrypted electronic content may only be accessed from the particular piece of media. The electronic content is only accessible from only the one piece of media having the unique identifier and is not accessible from any other media having a different or no identifier.

38 Claims, 10 Drawing figures

Previous Doc Next Doc Go to Doc#

L17: Entry 1 of 1 File: USPT Aug 13, 2002

DOCUMENT-IDENTIFIER: US 6434535 B1
**** See image for Certificate of Correction ****
TITLE: System for prepayment of electronic content using removable media and for prevention of unauthorized copying of same

Brief Summary Text (18):
According to a further feature, the step of communicating the electronic content to the piece of media, wherein the electronic content is in an encrypted format comprises encrypting at least one of the electronic content and an encryption key to the electronic content, the encrypting using the unique identifier as an encryption key. The electronic content is written to the one piece of media in an encrypted format using the unique identifier as a decryption key.

Brief Summary Text (30):
According to still another feature, the electronic content to be transmitted to the client device is encrypted using the unique identifier as an encryption key. The electronic content may be written to the piece of media in an encrypted format using the unique identifier as a decryption key.

Detailed Description Text (39):
According to the second embodiment of the present invention, the electronic data is encrypted during the download process to the media 28 using the unique identifier of the media 28, a vendor identifier and a user identifier as an encryption key. Such an encryption/decryption key will be identified herein as a "compound key." The encrypted protected electronic data is then associated to the media 28 by the compound key and may not be accessed from any other media. Thus, according to both embodiments, any protected electronic data that is copied from the destination media 28 to other storage devices will be unusable, as the other storage devices will at least not have the same unique identifier as the destination media 28. Such a system prevents unauthorized copying of the protected electronic data, protecting the intellectual property rights of the seller or owner of such rights. It is noted that other implementations are within the scope of the present invention, so long as the data written to the media 28 is protected from unauthorized copying.

Detailed Description Text (40):
The first embodiment proceeds from step 302 directly to step 304 (described below), however, the second embodiment performs additional steps by obtaining the necessary additional information to generate the compound key. As noted, the second embodiment provides for additional security by including not only the unique serial number in the encryption/decryption key, but also the vendor identifier and the user identifier. In particular, by using the compound key having vendor information and user information, certain additional safeguards may be built into the distribution of the protected data. The vendor information may be an identifier created by a third party vendor or industry group. The purpose of this identifier is to allow the vendor or an industry group to add additional layers of security to prevent unauthorized decryption of protected data by a person or software program not approved by the vendor or industry group. For example, as will be discussed below, the vendor information may be retrieved from application software running or

playing the protected content, thus further restricting use of the content to devices having licensed copies of the application software. Alternatively, the vendor information may retrieved from a server located on a local area network (LAN), wide area network (WAN), or the Internet, etc.

CLAIMS:

10. The method as recited in claim 9, wherein the electronic content is written to said one piece of media in an encrypted format using said unique identifier as a decryption key.

33. The system as recited in claim 32, wherein the electronic content is written to said piece of media in an encrypted format using said unique identifier as a decryption key.

Previous Doc Next Doc Go to Doc#

L16: Entry 1 of 1 File: USPT Aug 13, 2002

DOCUMENT-IDENTIFIER: US 6434535 B1
**** See image for Certificate of Correction ****
TITLE: System for prepayment of electronic content using removable media and for prevention of unauthorized copying of same

Abstract Text (1):
A system and method for distribution of electronic content over a network infrastructure and compensation of vendors of such data using prepaid media that includes a client device for operation by a user desiring to receive the electronic content and server that contains the electronic content and offering the electronic content for downloading to the client device via the network infrastructure. The client device communicates a unique identifier associated with a particular piece of media to which the electronic content is to be stored to the server. The server contacts a media tracking sever to determine if the media is valid and a remaining balance of the prepaid media. The cost of the electronic content to be downloaded is deducted from the remaining balance and credited to the vendor's account. The server then encrypts the electronic content using the unique identifier as a key and downloads the encrypted electronic content to the client computer, where the client computer writes the encrypted electronic content to the particular piece of media such that the encrypted electronic content may only be accessed from the particular piece of media. The electronic content is only accessible from only the one piece of media having the unique identifier and is not accessible from any other media having a different or no identifier.

Brief Summary Text (18):
According to a further feature, the step of communicating the electronic content to the piece of media, wherein the electronic content is in an encrypted format comprises encrypting at least one of the electronic content and an encryption key to the electronic content, the encrypting using the unique identifier as an encryption key. The electronic content is written to the one piece of media in an encrypted format using the unique identifier as a decryption key.

Brief Summary Text (20):
According to a feature of the invention, the step of transmitting the unique identifier to the vendor server further comprises accessing the one piece of destination media; reading the unique identifier from a predetermined location on the one piece of destination media; obtaining vender information; obtaining user information; building a compound key through a predetermined operation using the unique identifier, the vendor information, and the user information; and formatting the compound key into a first data structure for communication to the vendor server with the unique identifier.

Brief Summary Text (30):
According to still another feature, the electronic content to be transmitted to the client device is encrypted using the unique identifier as an encryption key. The electronic content may be written to the piece of media in an encrypted format using the unique identifier as a decryption key.

Brief Summary Text (31):
According to a further feature, the application software accesses the piece of destination media and reads the unique identifier from a predetermined location on the piece of destination media, obtains vender information, and obtains user information. The application software builds a compound key through a predetermined operation using the unique identifier, the vendor information, and the user information, and the application software formats the compound key into a first data structure for communication to the server with the unique identifier.

Detailed Description Text (4):
In accordance with the present invention, users (customers) purchase the removable media 28 for an amount that includes the price of the media 28 and an additional prepayment amount (e.g., $5, $10, $20, $50, or other) which may be used for purchasing and downloading of electronic content over the network infrastructure 12. The media 28 includes a unique identifier that is embedded on the media 28 such that it cannot be altered or copied. As customers select and download electronic content from vendors' servers 16c, the purchase price of such electronic content is deducted from the remaining balance of the media 28, which is associated to the media by the unique identifier by a tracking server 16a that maintains the balance for each unique identifier in a database. As will be described in detail below, the content is downloaded in an encrypted format to the media 28 using at least the unique identifier of the media 28 as an encryption key in order to prevent additional unauthorized copies from being made. Such a system provides a convenient mechanism for purchases of electronic content without the necessity of transmitting personal information or credit card numbers to the vendors. Further, the system of the present invention prevents unauthorized copying of the electronic content, as the content may only be accessed from the same piece of media 28 to which the content was downloaded because the encryption of the data will render the content unusable from other media 28 having a different or no unique identifier.

Detailed Description Text (20):
As will become evident to those of skill in the art, the features and aspects of the present invention may be implemented by any suitable combination of hardware, software and/or firmware. Referring now to FIG. 5, there is illustrated the process by which the media 28 is manufactured and the unique identifier and prepaid balance is established. The process begins at step 200 and the media 28 is assembled by the manufacturer at step 202 to construct the removable media disk 28. At step 204, the media is formatted using formatter 23 which formats the media 28 for use on the PC 20 and/or stand alone device 22 and also embeds the unique identifier (e.g., serial number) and an authentication code onto the media. The authentication code prevents hacking of serial numbers in that forging a serial number would statistically require 2.sup.64 attempts if the authentication code is a 64-bit number.

Detailed Description Text (21):
By way of a non-limiting example, the media 28 may comprise a ZIP.RTM. disk manufactured by Iomega Corporation, Roy, Utah. Each Iomega ZIP.RTM. disk contains a unique serial number that is written to a predetermined track during the formatting process which may be used as the unique identifier. The serial number is preferably created by but not limited to a pseudo random number generator. Further, while the media 28 has been described in terms of a ZIP.RTM. disk, it is not limited to the ZIP.RTM. disk, as the use of other removable media types having a unique serial number is within the scope and spirit of the present invention such as CD-R, DVD-RAM, and other removable floppy and hard disks. Further, it is not necessary for the assembly step (step 202) to occur contemporaneously with the formatting step (step 204). Nor do both steps need to be performed by the same manufacturing entity. In the case of the Iomega ZIP.RTM. disk, the formatter 23 may comprise a PC 20 having multiple standard ZIP.RTM. drives connected thereto. The formatter 23 ZIP.RTM. drives include firmware that allows writing of the unique serial number to a predetermined track that is not accessible by a standard ZIP.RTM. drive.

Detailed Description Text (22):
At step 206, the unique identifier and authentication code embedded onto the media are transmitted to the media tracking server 16a via e.g., TCP/IP sockets to an IP address of the media tracking server 16a in a predetermined data structure. Such a data structure may be as follows: struct SocketCommand { unsigned long Code; unsigned long Size; unsigned char Data[400]; };

Detailed Description Text (23):
The media tracking server 16a then stores the unique identifier and authentication code in a database. The database may include a relational database management program such as Oracle. At step 207, the prepaid value is determined, and in accordance with the invention may be established by the manufacturer or the tracking entity. For example, if the manufacturer sets the prepaid value, the value may be transmitted in the same data structure with the unique identifier and authentication code. The media tracking server 16a then parses the unique identifier, authentication code and predetermined value before entering them into the tracking database. If the media tracking server 16a sets the prepaid value, then the tracking server 16a sends a response back to the manufacturer server 16b containing the prepaid value such that the media 28 may be properly labeled for sale.

Detailed Description Text (27):
Referring to FIG. 6, there is illustrated the process of activating the media 28 for use by consumers. The process begins a step 220 where the user inserts the prepaid media 28 into the media drive 52 (step 222). An application running on the PC 20 (or stand alone device 22) reads the unique identifier and authentication code (step 224). This is performed by querying the media using an application programming interface (API) such as the Iomega Ready API, or other suitable method.

Detailed Description Text (29):
It can be appreciated that the unique serial number is not limited to information stored on the media 28, such as the serial number, and that other types of information could be used as the unique identifier. In addition, the unique serial number should contain a sufficient number of bits (length) to ensure that no two pieces of media have the same identifier. For example, each Iomega ZIP.RTM. disk contains a unique 39 byte (312 bits) serial number, and other bit lengths may be utilized.

Detailed Description Text (30):
Alternatively, at step 224 the software may collect additional information from the user, such as name, address, telephone number, e-mail address, etc. together with the unique identifier, which may be transmitted to register the media 28 if requested by the tracking entity.

Detailed Description Text (38):
Two alternative embodiments for the selection/download process are contemplated in accordance with the present invention. As will be described in detail below, in accordance with one embodiment of the present invention, the electronic data is encrypted during the download process to the media 28 using only the unique identifier (e.g., serial number) of the media 28 as an encryption key. The encrypted protected electronic data is then associated to the media 28 by the unique identifier and may not be accessed from any other media having a different or no unique identifier.

Detailed Description Text (39):
According to the second embodiment of the present invention, the electronic data is encrypted during the download process to the media 28 using the unique identifier of the media 28, a vendor identifier and a user identifier as an encryption key. Such an encryption/decryption key will be identified herein as a "compound key."

The encrypted protected electronic data is then associated to the media 28 by the compound key and may not be accessed from any other media. Thus, according to both embodiments, any protected electronic data that is copied from the destination media 28 to other storage devices will be unusable, as the other storage devices will at least not have the same unique identifier as the destination media 28. Such a system prevents unauthorized copying of the protected electronic data, protecting the intellectual property rights of the seller or owner of such rights. It is noted that other implementations are within the scope of the present invention, so long as the data written to the media 28 is protected from unauthorized copying.

Detailed Description Text (40):
The first embodiment proceeds from step 302 directly to step 304 (described below), however, the second embodiment performs additional steps by obtaining the necessary additional information to generate the compound key. As noted, the second embodiment provides for additional security by including not only the unique serial number in the encryption/decryption key, but also the vendor identifier and the user identifier. In particular, by using the compound key having vendor information and user information, certain additional safeguards may be built into the distribution of the protected data. The vendor information may be an identifier created by a third party vendor or industry group. The purpose of this identifier is to allow the vendor or an industry group to add additional layers of security to prevent unauthorized decryption of protected data by a person or software program not approved by the vendor or industry group. For example, as will be discussed below, the vendor information may be retrieved from application software running or playing the protected content, thus further restricting use of the content to devices having licensed copies of the application software. Alternatively, the vendor information may retrieved from a server located on a local area network (LAN), wide area network (WAN), or the Internet, etc.

Detailed Description Text (46):
Alternatively, the Data field may comprise a plurality of fields containing the customer information, billing information, the unique serial number, the vendor identifier and the user identifier as parsed fields. The data field may be formatted to have the following data structure: { char First[20]; char Last[20]; char Address[40]; char City[20]; char State[3]; char Zip[6]; char CreditCard[17]; char ExpDate[5]; char Phone[13]; char Serial[40]; char Compound[40]; long int DataID; };

Detailed Description Text (50):
During the download process, the server 16 encrypts the data key for the electronic content and/or the electronic content using the unique identifier (first embodiment) or the compound key (second embodiment) as an encryption key (step 318). Additional information may be used in the encryption key, such as the customer information, etc. for additional security. While any suitable encryption algorithm may be utilized at step 318, the data encryption is preferably performed using the well known Blowfish encryption algorithm. The Blowfish encryption algorithm is advantageously fast, especially when implemented on 32-bit microprocessors with large data caches, such as the Intel Pentium and the IBM/Motorola PowerPC. Briefly, Blowfish is a variable-length key, 64-bit block cipher which may be implemented in either hardware or software. The algorithm consists of two parts: a key-expansion part and a data-encryption part. The key expansion part converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. The data encryption occurs via a 16-round Feistel network, wherein each round consists of a key-dependent permutation and a key- and data-dependent substitution. All operations are exclusive ORs (XOR) and additions on 32-bit words. The only additional operations are four indexed array data lookups per round to generate the encrypted data.

Detailed Description Text (56):
Referring now to FIG. 9, there is illustrated the error process that occurs if an

error occurs during the download of the electronic content to the media 28. The process begins at step 450 after the error is encountered, and the E-commerce server 16c sends an error code via TCP/IP sockets and an appropriate data structure to the application software on the PC 20. The application software prompts the user with an error message and determines if the error is a disk full error at step 456. If the error is a disk full error, then at step 458 the user is prompted to insert a new prepaid media disk 28 at step 458. At step 459, the unique identifier of the new media is read (see process of step 302), and if operating in accordance with the second embodiment, the functions of steps 302A, 302B and 302C are also performed to build compound key. The newly inserted media is then activated in accordance with steps 226 and 228. Next, the media tracking server 16a is contacted at step 460 such that the balance (if any) remaining on the full disk is transferred to the new disk and the process jumps to step 306 of FIG. 7.

Detailed Description Text (60):
It is further noted that the E-commerce server 16c may store digital content to be downloaded in an encrypted or unencrypted format. If the digital content to be downloaded is not stored in an encrypted format, then it is preferably encrypted upon downloading using the unique serial number or compound key as an encryption key. If the digital content to be download is stored on the server 16 in an encrypted format (pre-encrypted) prior to downloading then the server would need only encrypt the data key to the content (i.e., the software application, music or video). Pre-encryption may be preferable to provide greater performance in environments where large amounts of data need to be encrypted per transaction. Such electronic distribution systems may be heavily burdened if they were required to encrypt the entire content that is to be electronically distributed. However, it may be preferable to double encrypt the downloaded content at step 308 by encrypting the pre-encrypted content and the data key to the pre-encrypted content using the unique serial identifier or compound key (and any additional information) as an encryption key. Such a technique would greatly increase the security of the data to be transmitted, as the data may be double encrypted prior to transmission to the client, as noted above. While the process at step 318 has identified encrypting the data key or the data key and the content, it is also possible that at step 318 that only the content to be transmitted is encrypted using the unique serial number or compound key as a key. If enhanced security is a concern, additional transaction information such as the purchaser's name, address, credit card number, etc. may be included with the content.

Detailed Description Text (61):
The present invention advantageously utilizes the unique identifier of the media as an encryption key which allows any electronic data to be protected against copying. Additionally, by using the unique identifier of the media, rather than a hardware device, the protected electronic data may be read/played on any device capable of reading the media. Thus, the protected electronic data becomes portable and is tied only to a single removable media, allowing the protected electronic data to be shared while preventing the protected electronic data from being copied and read/played from another media. Further, present invention may be used in a single encryption method or multiple encryption method where the key to the protected electronic data itself is encrypted using the serial number of the disk as the key.

CLAIMS:

1. A method of distributing electronic content from a vendor server to a client device via a network infrastructure which includes a Transmission Control Protocol/Internet Protocol Network and for payment to a vendor of the electronic content, said method utilizing a permanent unique identifier stored on a piece of destination media on which the electronic content is to be stored to associate the electronic content with only said piece of media and utilizing a predetermined value stored on said piece of media as payment for the electronic content, said

method comprising: contacting the vendor server via the network infrastructure; transmitting said unique identifier of said piece of destination media to the vendor server; communicating, via said network infrastructure information from said vendor server to media tracking server to determine if said unique identifier is valid and to determine a remaining balance of said predetermined value of said piece of media; encrypting said electronic content into an encrypted format having said unique identifier as a key; communicating, via the network infrastructure, said encrypted format of said electronic content to said piece of media; and writing the electronic content to said piece of media in accordance with said unique identifier such that the electronic content may be accessed for use from only said piece of media having said unique identifier.

9. The method as recited in claim 7, wherein said communicating the electronic content to said piece of media, wherein the said electronic content is in an encrypted format comprises encrypting at least one of the electronic content and an encryption key to the electronic content, said encrypting using said unique identifier as an encryption key.

10. The method as recited in claim 9, wherein the electronic content is written to said one piece of media in an encrypted format using said unique identifier as a decryption key.

15. The method as recited in claim 2, wherein said transmitting said unique identifier to the vendor server further comprises: accessing said one piece of destination media; reading said unique identifier from a predetermined location on said one piece of destination media; obtaining vender information; obtaining user information; building a compound key through a predetermined operation using said unique identifier, said vendor information, and said user information; and formatting said compound key into a first data structure for communication to the vendor server with said unique identifier.

23. The method as recited in claim 1 wherein said piece of media is a removable magnetic disk and said unique identifier is the serial number of said disk.

24. A system for distribution of electronic content over a network infrastructure which includes a Transmission Control Protocol/Internet Protocol Network to a client device running an application program, said client device including a piece of media having a permanent unique identifier and a prepaid monetary value inserted therein, said system further compensating a vendor of the electronic content from a remaining balance of said prepaid monetary value, said system comprising: a vendor server containing the electronic content and offering the electronic content for downloading to said client device via said network infrastructure; a media tracking server that maintains said remaining balance of said piece of media in accordance with said unique identifier; wherein said unique identifier is communicated to said vendor server and said vendor server communicates said unique identifier to said media tracking server to determine said remaining balance, and wherein said vendor server encrypts the electronic content with said unique identifier as a key and downloads the encrypted electronic content to said piece of media such that the electronic content may only be accessed from said piece of media.

32. The system as recited in claim 30, wherein the electronic content to be transmitted to the client device is encrypted using said unique identifier as an encryption key.

33. The system as recited in claim 32, wherein the electronic content is written to said piece of media in an encrypted format using said unique identifier as a decryption key.

34. The system as recited in claim 25, wherein said application software accesses said piece of destination media and reads said unique identifier from a

predetermined location on said piece of destination media, obtains vender information, and obtains user information, wherein said application software builds a compound key through a predetermined operation using said unique identifier, said vendor information, and said user information, and wherein said application software formats said compound key into a first data structure for communication to the server with said unique identifier.

38. The system as recited in claim 24 wherein said piece of media is a removable magnetic disk and said unique identifier is the serial number of said disk.

Previous Doc Next Doc Go to Doc#

288. (Previously presented) The method of claim 280 wherein the license request is contained in an HTTP request transmitted by the client computer to an address identified by the digital content.

289. (Previously presented) The method of claim 280 wherein the license request includes a version number for a Digital Rights Management (DRM) system on the client computer.

290. (Currently Amended) A method for a server to provide to a client computer a digital license of one or more rights to render digital content, the digital content encrypted with a decryption key, the method comprising:

receiving, from the client computer, a license request, the license request containing a key identifier that identifies the decryption key and a client certificate associated with the client computer, the client certificate including a public key associated with the client computer; and

responsive to the request, transmitting a license response to the client computer, the license response including a digital rights license, the decryption key identified by the key identifier, and at least one server certificate to be used by the client computer to validate the license response,

wherein the transmitting further comprises transmitting the decryption key as an encrypted decryption key, the encrypted decryption key being the decryption key encrypted with the public key, the decryption key being produced by application of the key identifier as an input to an algorithm by which the decryption key is produced.

291. (Previously presented) The method of claim 290 wherein the license request includes a content identifier, and a list containing one or more requested